BlackBerry Enterprise Server for IBM Lotus Domino

Version 4.0

Handheld Management Guide

BlackBerry Enterprise Server Version 4.0 for IBM Lotus Domino Handheld Management Guide

Last modified: 10 November 2004

Part number: SWD_BES(EN)-007.001

At the time of publication, this documentation complies with BlackBerry Enterprise Server Version 4.0 for IBM Lotus Domino.

© 2004 Research In Motion Limited. All rights reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, BlackBerry and ' Always On, Always Connected' are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion is under license. IBM, Lotus, and Domino are trademarks of International Business Machines Corporation in the United States, other countries, or both. Java and J2ME are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. or other countries. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

The BlackBerry handheld and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current listing of applicable patents.

This document is provided " as is" and Research In Motion Limited (RIM) assumes no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS, OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN, OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS AFFILIATED COMPANIES AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information and/or third-party web sites (" Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation, the content, accuracy, copyright compliance, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the third party in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses, and terms and conditions are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.

Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server Software, BlackBerry Desktop Software, and/or BlackBerry Handheld Software and may require additional development or third-party products and/or services for access to corporate applications. Prior to subscribing to or implementing any third-party products and services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third-party products and services. Installation and use of third-party products and services with RIM' s products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for acquiring any such licenses. To the extent that such intellectually property licenses may be required, RIM expressly recommends that you do not install or use these products until all such applicable licenses have been acquired by you or on your behalf. Your use of third-party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third-party products and services that are provided with RIM' s products and services are provided " as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the third-party products or services and RIM assumes no liability whatsoever in relation to the third-party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/) and/or licensed pursuant to Apache License, Version 2.0 (http://www.apache.org/licenses/). For more information, see the NOTICE.txt file included with the software.

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an " AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House, 36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada

Contents

1 Configuring the BlackBerry Handheld Management environment 9

Communication ports 9

Define handheld connection settings 9

Configure the ports 10

BlackBerry Desktop Software 10

Desktop Software configurations 10

Configuring the BlackBerry Desktop Software installation files 11

Extract the installation files 11

Copy the installation files to a network directory 11

Configure the installation options 11

Run the Desktop Software installation in silent mode 12

Running the Desktop Manager in record mode 13

Distribute Desktop Software to user computers 14

View Desktop Software installation log files on user computers 14

2 Deploying handhelds 15

Deployment process 15

Selecting a deployment method 15

Defining Handheld Software configurations 16

Set a software configuration 16

Enabling email prepopulation 17

Configure email prepopulation for a user 17

Deploying handhelds using the administration computer 18

Assign a software configuration to a user 18

Assign a handheld to a user 18

Deploying handhelds wirelessly 19

Sending PIM data using the BlackBerry Router 19

Enable a user to perform a wireless activation 20

Deploying handhelds using the Desktop Manager 20

3 Administering handhelds 21

Managing handheld information reporting 21

Configure handheld information management 21

View handheld status information from the configuration database 21

View handheld status information from the handheld 22

Retrieve handheld status information 22

Export handheld status information 22

Set handheld owner information 22

Controlling Handheld Software applications 23

Define which applications are installed on handhelds 23

Controlling third-party software applications 23

Define IT policies for third-party applications 24

Viewing the status of IT policy changes 24

Sending IT policies to handhelds ... 25
Define application control policies ... 25
Assign application control policies to software configurations ... 25
Manage application control policies ... 26
Send third-party software applications to handhelds wirelessly ... 26
Managing software configurations ... 27
Modify a software configuration ... 27
Delete a software configuration ... 27
Copy a software configuration ... 27
Unassign a software configuration from a user ... 27
Check the status of Handheld Software and third-party applications on a handheld ... 28
Handheld security ... 28
Manage handheld security ... 29
Managing activation passwords ... 29
Reset an activation password ... 30
Expire an existing activation password ... 30
Issuing new handhelds to users ... 30
Activate a new handheld ... 31
Issuing existing handhelds to new users ... 31
Switch the user account on the handheld ... 31

4 Upgrading handhelds ... 33
Selecting an upgrade method ... 33
Configuring Handheld Software on an administration computer ... 34
Install Handheld Software ... 34
Configure required software ... 35
Create the software index ... 35
Share Handheld Software and upgrade tools ... 35
Upgrading Handheld Software ... 36
Upgrade handhelds using the administration computer ... 36
Upgrade handhelds using the Application Loader ... 37
Forcing upgrades to handhelds using the Desktop Manager ... 37

Appendix A: Exported handheld properties ... 39
Handheld hardware components ... 39
Handheld software components ... 39
Component capabilities ... 40
Status ... 40
Service books ... 41
Software applications ... 41
Modules ... 41

Appendix B: Software application control ... 43
Application control policy properties ... 43
Sample application control policies ... 43
Sample software configurations ... 44

Appendix C: Wireless backup and restore 45
Data that is not backed up wirelessly 45
Backup and restore handheld data 45
Backup handheld data using the Application Loader 46

1

Configuring the BlackBerry Handheld Management environment

- Communication ports
- BlackBerry Desktop Software
- Configuring the BlackBerry Desktop Software installation files

Communication ports

To deploy and maintain BlackBerry Wireless Handhelds™ that have a serial connection to the BlackBerry® Manager, you must enable the ports to which they are connected. Handhelds that have a USB connection are detected automatically when connected to the computer, and they appear in the BlackBerry Manager Ports window.

Note: Do not enable ports to which other devices are connected.

Define handheld connection settings

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, on the **Tools** menu, click **Options**.
3. Click **Serial Ports**.
4. In the **COM1** and **COM2** sections, perform one of the following actions:

Action	Procedure
Enable the port.	▸ From the drop-down list, select **True**.
Set the port speed.	▸ From the drop-down list, select a speed.
Support a USB to serial adapter connection.	▸ From the drop-down list, select **True**.

5. Click **OK**.

If the software cannot detect the handheld on a COM port or USB port, the **"There are no connected handhelds"** message displays. Verify that the handheld and cradle cable or the USB cable appears to be connected securely, and that no other handhelds are sharing the port.

Note: If the handheld is connected to the computer on which the BlackBerry Manager is installed, when you open a user's Properties window, a message prompts you to assign the handheld to that user.

Configure the ports

1. In the BlackBerry Manager, in the left pane, click **Ports**.
2. In the **Connection** list, click a port.
3. Click **Configure Port**.
4. Perform one of the following actions:

Action	Procedure
Enable a port.	1. Click **Enabled**. 2. From the drop-down list, select **True**.
Disable a port.	1. Click **Enabled**. 2. From the drop-down list, select **False**.
Set the port speed.	1. Click **Port Speed**. 2. From the drop-down list, select a port speed.
Support a USB to serial adapter connection.	1. Click **USB to serial adapter support**. 2. From the drop-down list, select **True**. **Note:** USB to serial adaptor connections can be problematic. Research In Motion recommends not using USB to serial adapter connections.

5. Click **OK**.

BlackBerry Desktop Software

You can distribute the BlackBerry Desktop Software version 4.0 to user computers to maintain handhelds without administering the handhelds from the administration computer. Using the Desktop Software components to upgrade BlackBerry Handheld Software and transfer data from the messaging and collaboration server to handhelds decreases the use of the wireless network.

Obtain the BlackBerry Desktop Software installation files from the BlackBerry Desktop Software installation CD, from your service provider, or by visiting www.blackberry.com/support.

Desktop Software configurations

There are three Desktop Software version 4.0 configurations that you can push to user computers.

Desktop Software configurations	Description
BlackBerry Handheld Manager	• allows data transfer using the BlackBerry Router instead of over the wireless network when the handheld is connected to the user computer • allows handheld application data to be backed up and restored when upgrading Handheld Software using the BlackBerry Application Loader • displays statistics on the user computer of data transferred using the BlackBerry Router while bypassing the wireless network • tracks data transfer through the network to show wireless data transfer savings using the BlackBerry Router

Desktop Software configurations	Description
Handheld Manager and BlackBerry Desktop Manager	• includes all Handheld Manager capabilities • enables email reconciliation and synchronization of personal information management (PIM) data when the handheld is connected to the user computer • includes the Application Loader tool to install on user computers • includes Handheld Software upgrade installation files, which can be distributed to user computers or maintained on the administration computer • enables you to force Handheld Software upgrades onto handhelds
Handheld Manager, Desktop Manager, and Certificate Synchronization	• includes all Handheld Manager and Desktop Manager capabilities • provides the ability to synchronize PKI certificates to Java™-based handhelds • uses the BlackBerry Desktop Software with S/MIME support software

Configuring the BlackBerry Desktop Software installation files

You can create and set the installation options for the Desktop Software and the optional Handheld Software installation files for a correct installation. You can configure the Desktop Software installation files to install different Desktop Software configurations on user computers. You can also record the Desktop Manager to define and configure settings in the Desktop Manager application.

You can either configure the installation to enable users to interact with the installation or push a completely silent installation. See "Run the Desktop Software installation in silent mode" on page 12 for more information.

Extract the installation files

Note: The installation files are already extracted on the BlackBerry Desktop Software installation CD. If you are using a CD for the installation, skip to "Copy the installation files to a network directory" on page 11.

1. Create an installation directory on the administration computer.
2. Click the **.exe** file, and then extract the installation files to the directory that you created in step 1.
3. When prompted to install the BlackBerry Desktop Software, click **Cancel**.

Copy the installation files to a network directory

1. Copy the installation files to a network directory.
2. If you do not want to maintain the Handheld Software in a shared software directory, create a folder named "Device" in the network directory.
3. Add all of the required Handheld Software installation files to the Device folder that you created in step 2.

Configure the installation options

You can remove options from the installation. For example, if users use a IBM® Lotus® Domino® messaging and collaboration server, then remove the option to install any Microsoft® Exchange Desktop Software settings.

1. Open the **setup.ini** file.

2. At the bottom of the setup.ini file, add an **[INSTALL_OPTIONS]** tag. See the install.txt file on the BlackBerry Desktop Software installation CD for an example of [INSTALL_OPTIONS].
3. Add installation options after the [INSTALL_OPTIONS] tag, and then configure the options.

Installation option	Action	Default
COUNTRY	Specify the countries to display the software licence agreement for. **Note:** See the install.txt file on the BlackBerry Desktop Software installation CD for the latest list of countries with software licence agreements.	United States
SETUPTYPE	Specify if the setup type is **Enterprise** or **Internet**.	Enterprise
MAILSERVER	Specify if **Exchange**, **Lotus**, or **GroupWise** is the messaging and collaboration server used by the user.	Exchange
REDIRECTOR	Specify if the **Desktop** or **Enterprise** controls email redirection.	Enterprise
USERS	Specify if **AllUsers** or **CurrentUser** have access to the Desktop Software.	AllUsers
SHORTCUTSTARTUP	Specify whether to add a Desktop Software shortcut to the Start menu.	False
SHORTCUTDESKTOP	Specify whether to add a Desktop Software shortcut to the desktop.	False
HANDHELDINSTALLERDIR	Specify the path to the Handheld Software installation files if you do not want to maintain Handheld Software in a shared software directory.	Device folder in the network directory (*<drive:\network directory>*\Device)
UNINSTALLEXISTINGHANDHELDS	Specify whether to remove existing Handheld Software bundles during the installation.	False
SUPPRESSREBOOT	Specify whether to suppress any reboots that might occur during the installation.	False

Note: If there are conflicting configurations, the hierarchy of settings determines how to resolve the conflict. For example, if the **SETUPTYPE** option is set to **Internet** and the **REDIRECTOR** option is set to **Enterprise**, then the **REDIRECTOR** setting is ignored.

4. Save the **setup.ini** file to the same location in which the setup.exe file resides.

Run the Desktop Software installation in silent mode

- At the command prompt, type ***<drive:\network directory>*\setup.exe /s /l*<*language ID*>* */v"INSTALLLEVEL=*<*install level ID*>*"** where *<drive:\network directory>* specifies the network directory, *<language ID>* specifies a language other than English, and *<install level ID>* specifies a Desktop Software configuration.

Language	Language ID
French	1036
German	1031
Italian	1040
Spanish	1034

Desktop Software configuration	Installation level ID
Handheld Manager only	1
Handheld Manager and Desktop Manager	100 (default)
Handheld Manager, Desktop Manager, and Certificate Synchronization	125

Note: If you do not specify /l in the silent installation, English, the default language, is installed. If you do not specify /v in the silent installation, the default installation level is used.

Running the Desktop Manager in record mode

If you use the Desktop Manager in your Desktop Software configuration, and the Desktop Manager is installed locally, you can run the Desktop Manager in record mode. Running the application in record mode enables you to define Desktop Software settings and export them to .xml files, which you can deploy to user computers. The Desktop Software configuration settings that you define are applied when the Desktop Software is installed on a user computer on which there is no existing Desktop Manager.

Notes: The .xml files that you generate must reside in the network installation directory for the Desktop Software to successfully apply them during the Desktop Software installation.

If you specify the Desktop Manager in your Desktop Software configuration, Research In Motion recommends that you configure the installation options. See "Configure the installation options" on page 11 for more information.

Configure the Desktop Manager settings

1. At the command prompt, switch to the local directory in which the Desktop Manager is installed.
2. Run the Desktop Manager by typing **DesktopMgr.exe /r** *<drive:\ network directory>* where *<drive:\ network directory>* specifies the network directory.
3. In the Desktop Manager, configure the default settings to apply to user computers.

Tool	Action
Desktop Manager	1. Click **View**, and then specify the menu settings. 2. Click **Options**, and then specify the menu settings. 3. Double-click **Backup and Restore**. 4. Click **Options**, and then specify the component settings.
Redirector Settings	1. Double-click **Redirector Settings**. 2. On the **General** tab, specify the component settings. 3. On the **Filters** tab, specify the component settings. 4. On the **Security** tab, specify the component settings. 5. On the **Advanced** tab, specify the component settings. 6. Click **OK**.
Intellisync	1. Double-click **Intellisync**. 2. In the **Synchronize now** section, specify the synchronization settings. 3. Click **Configure email**, and then specify the component settings. 4. Click **Configure PIM** > **Choose**, and then specify the component settings. 5. Click **Configure PIM** > **Configure** > **Advanced Settings**, and then specify the component settings. 6. Click **Auto start**, and then specify the component settings. 7. Click **Close**. **Note:** Intellisync is not used when wireless PIM synchronization is enabled for a user.

4. To write the settings to the .xml files, close the Desktop Manager.
5. Verify that the .xml files appear in the network directory where the setup.exe file resides.

File name	Related tool
DefaultDesktop.xml	Desktop Manager
DefaultRedirectorSettings.xml	Redirector Settings

File name	Related tool
DefaultIntellisync.xml	Intellisync

Distribute Desktop Software to user computers

- Use your preferred distribution method to push the configured Desktop Software installation program from the network directory to user computers.

When the Desktop Software installation program runs in silent mode, users see a progress bar, but they do not interact with the installation. Any Handheld Software installation files that you specified in the [INSTALL_OPTIONS] tag section in the setup.ini file open and a progress bar displays on user computers while the Handheld Software is installing on handhelds.

View Desktop Software installation log files on user computers

Log files are generated automatically and stored on user computers in a temporary directory.

1. On the user computer, in the taskbar, click **Start** > **Run**.
2. Type **%TEMP%**.
3. Open **BB_*<prefix>*.log**, where *<prefix>* specifies a Desktop Software and Handheld Software installation component.

2

Deploying handhelds

- Deployment process
- Selecting a deployment method
- Defining Handheld Software configurations
- Enabling email prepopulation
- Deploying handhelds using the administration computer
- Deploying handhelds wirelessly
- Deploying handhelds using the Desktop Manager

Deployment process

To deploy handhelds successfully, you must complete the following actions:

Action	Procedure
Install Handheld Software on the handheld if the desired version is not installed on the handheld.	▸ See "Configuring Handheld Software on an administration computer" on page 34 and "Upgrading Handheld Software" on page 36 for more information.
Provision or activate the handheld by performing one of the following actions: • assign the handheld to a user • install service books on the handheld	▸ See " Selecting a deployment method" on page 15 for more information.
Populate the handheld with previously received email messages.	▸ See " Enabling email prepopulation" on page 17 for more information.
Synchronize PIM data on the handheld.	▸ See " Selecting a deployment method" on page 15 for more information.

Selecting a deployment method

You can deploy handhelds using the administration computer, wirelessly, or using the Desktop Manager. If you deploy a handheld using the administration computer, the handheld must be connected to the administration computer.

If you deploy a handheld wirelessly or using the Desktop Manager, the handheld does not have to be in your possession during the deployment process.

Deployment option	Uses and advantages	Limitations
deploy handhelds using the administration computer	• provides complete control over the initial handheld activation and personal information management (PIM) synchronization processes • assign software configurations to users and load software configurations onto handhelds • initial load of PIM data is transferred from the administration computer to the handheld using a serial or USB connection • load Handheld Software applications onto handhelds during the initial deployment process	• the number of handhelds that you can deploy at one time is limited to the number of communication ports that are on the administration computer • handhelds must be in your possession and connected to the administration computer on which the BlackBerry Manager is installed

Deployment option	Uses and advantages	Limitations
deploy handhelds wirelessly	• deploy handhelds without a physical connection to the administration computer • deploy handhelds that are not connected to user computers • users can purchase handhelds and activate them while they are away from their computers • direct the initial load of PIM data onto handhelds over the wireless network or using the BlackBerry Router • deploy multiple handhelds at one time • load Handheld Software applications onto handhelds during the initial deployment process using the Application Loader	• cannot control software applications loaded onto handhelds • must communicate the activation password to the user, which might cause errors during the deployment process • directing the initial load of PIM data onto handhelds over the wireless network can use up significant bandwidth
deploy handhelds using the Desktop Manager	• deploy handhelds without a physical connection to the administration computer • initial load of PIM data is transferred from the user computer to the handheld using a serial or USB connection	• the Desktop Manager must be installed on user computers before deploying handhelds • handhelds must be connected to user computers during the deployment process • cannot control software applications loaded onto handhelds

Defining Handheld Software configurations

You define software configurations to load Handheld Software applications using the BlackBerry Manager, to assign application control policies to users, to send and administer third-party software applications on handhelds, and to make sure that the most current version of Handheld Software is running on handhelds. Software configurations create more uniformity between the software applications that are installed on handhelds and require less interaction with the BlackBerry Manager when installing software applications on handhelds.

To set a software configuration for a handheld, you must install the Handheld Software associated with that handheld on the administration computer and share the location where the Handheld Software resides. See "Install Handheld Software" on page 34 and "Share Handheld Software and upgrade tools" on page 35 for more information.

Set a software configuration

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. Click **Add New Configuration**.
3. In the **Configuration Name** field, type a name.
4. In the **Configuration Description** field, type a description.
5. Define the location of the Handheld Software by clicking **Change**.
6. Specify the location of the Handheld Software. For example, *<shared computer name>*\Research In Motion\.
7. Click **OK**.
8. In the **Applications List**, select the check box beside the handheld series to configure Handheld Software for.
9. Expand the handheld series Handheld Software application tree.

10. Perform one of the following actions:

Action	Procedure
Install applications on handhelds.	▸ Select the check box beside the application.
Do not install applications on handhelds or remove applications from handhelds.	▸ Clear the check box beside the application.

Note: You can configure required Handheld Software applications so that they appear available or unavailable in the Handheld Software Configuration screen. See "Configure required software" on page 35 for more information.

11. Click **Policies** to define application control policies for any third-party software applications. See "Define application control policies" on page 25 for more information.
12. From the **Policy** drop-down list, select an application control policy for the selected third-party applications.

Note: Application control policies can be assigned only to Java-based handhelds that are running Handheld Software version 4.0.

13. Click **OK**.

Enabling email prepopulation

The BlackBerry Enterprise Server™ populates previously received email messages automatically onto a handheld when a new handheld is deployed to a user if the handheld is running Handheld Software version 4.0. The maximum number of days to go back (from the present day) to prepopulate email messages is 7, and the maximum number of email messages that can be populated on the handheld is 350.

Email prepopulation adheres to the email filter rules and folder redirection settings, including the Sent Items folder, specified in the user's Desktop Manager or in the BlackBerry Manager when prepopulation starts.

When email pre-population is enabled, users might receive duplicate email messages in the following situations:

- If a user receives a replacement handheld and restores backed up email messages from the previous handheld, the user receives duplicate email messages on the new handheld within the specified range of the email prepopulation settings.
- If you remove a user from the BlackBerry Enterprise Server, then re-add the same user to the BlackBerry Enterprise Server, and then the user deploys their existing handheld, the user receives duplicate email messages on the handheld.

You can disable email prepopulation if a user received a replacement handheld and backed up their previously received email messages on their computer.

Configure email prepopulation for a user

1. In the BlackBerry Manager, click a server.
2. On the **Server Configuration** tab, click **Edit Properties.**
3. Click **Email**.

4. In the **Email Pre-population** section, perform one of the following actions:

Field	Description
Set the number of days to go back to prepopulate email messages upon.	▸ In the **Prepopulation By Message Age** field, set the number of days to go back.
Set the maximum number of email messages to prepopulate.	▸ In the **Prepopulation By Message Count** field, set the total number of messages.
Turn email prepopulation off.	▸ In the **Prepopulation By Message Age** field, type **0**.

5. Click **OK**.

Deploying handhelds using the administration computer

You can deploy handhelds by connecting them to the administration computer. This method enables you to control the activation and initial deployment of multiple handhelds. You can also upgrade the Handheld Software before deploying the handheld to a user. See "Upgrade handhelds using the administration computer" on page 36 for more information.

Assign a software configuration to a user

1. In the BlackBerry Manager, in the left pane, click **Handhelds**.
2. In the **User Name** list, click the user to assign the software configuration to.

   Tip: To select multiple users, hold CTRL.

3. Click **Assign Software Configuration**.
4. Click the software configuration to assign.
5. Click **OK**.

Assign a handheld to a user

Assigning a handheld to a user associates the handheld with the user's email account and installs service books on the handheld.

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click **Handhelds**.
3. In the **User Name** list, click the user to assign to the handheld.
4. Click **Assign Handheld to User**.
5. Click the handheld to assign to the user.
6. Click **OK**.

Deploying handhelds wirelessly

You can deploy handhelds using the BlackBerry Manager by sending wireless activation passwords to users. After an activation password has been entered on a handheld, it becomes inactive and subsequent passwords for the same user must be reset or resent to the handheld. Accented characters are not supported in activation passwords. You can configure whether users must connect their handhelds to their computer during the deployment process or carry out the deployment process wirelessly using PIM synchronization IT policies.

Sending PIM data using the BlackBerry Router

To save bandwidth, you can prevent the transfer of data to the handheld during the handheld deployment process unless a connection to the BlackBerry Router is established. By default, the BlackBerry Enterprise Server sends the initial bulk load of data during handheld deployment over the wireless network.

To send PIM data using the BlackBerry Router, the Handheld Manager must be installed on user computers. During the handheld deployment process, the Handheld Manager connects to the BlackBerry Router to receive data. To receive data using the BlackBerry Router, users must connect their handheld to their computer. If the connection to the BlackBerry Router is interrupted, the transfer of data during the handheld deployment process continues over the wireless network.

Configure PIM synchronization IT policies

1. In the BlackBerry Manager, on the **Global** tab, click **Edit Properties**.
2. Click **IT Policy**.
3. In the **IT Policy Administration** section, double-click **IT Policies**.
4. Perform one of the following actions:

Action	Procedure
Add a rule to the default IT policy and send the modified default IT policy to users.	1. From the list of policies, click **Default**. 2. Click **Properties**. 3. Click **PIM Sync Policy Group**. 4. Click the **Disable Wireless Bulk Loads** policy rule. 5. From the drop-down list, select **True**. 6. Click **OK**.
Create a new IT policy, add users to the new policy, and send the policy to users.	1. Click **New**. 2. Type a policy name. 3. Click **PIM Sync Policy Group**. 4. Click the **Disable Wireless Bulk Loads** policy rule. 5. From the drop-down list, select **True**. 6. In the **IT Policy Administration** section, double-click **IT Policies**. 7. In the left pane, click a user. 8. In the right pane, click the new policy. 9. Click **OK**.

Enable a user to perform a wireless activation

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. In the lower pane, expand **Service Access**.
4. Perform one of the following actions:

Action	Procedure
Generate the activation password and send the activation password automatically to the user in an email message.	▸ Click **Generate and Email Wireless Activation Password**. The user receives an email on their computer that provides the activation password. **Note:** The expiration time is set to 48 hours by default.
Define the activation password and set the password expiration time.	1. Click **Set Activation Password**. 2. Type a shared secret password. 3. Retype the password to confirm it. 4. From the **Password Expires in** drop-down list, select an expiration time. 5. Click **OK**. 6. Notify the user of the new password.

Note: The shared secret password is specific to a user account. The password expires after the specified expiration time (48 hours by default when generated automatically) or five unsuccessful password entry attempts on the handheld.

Deploying handhelds using the Desktop Manager

You can deploy handhelds by connecting them to user computers that have the Desktop Manager installed. You can distribute the BlackBerry Desktop Software version 4.0 to user computers to maintain handhelds without administering them from the administration computer. See " BlackBerry Desktop Software" on page 10 for more information.

1. Configure the Desktop Software installation files to install the Desktop Manager component. See " Configuring the BlackBerry Desktop Software installation files" on page 11 for more information.
2. Push the Desktop Software to user computers. See " Distribute Desktop Software to user computers" on page 14 for more information.
3. Inform users to start the Desktop Manager and connect their handhelds to their computers.

3

Administering handhelds

- Managing handheld information reporting
- Controlling Handheld Software applications
- Controlling third-party software applications
- Managing software configurations
- Handheld security
- Managing activation passwords
- Issuing new handhelds to users
- Issuing existing handhelds to new users

Managing handheld information reporting

You can enable or disable automatic handheld management for a user. If the setting is enabled for a user, the current handheld status information is sent to the administration computer during a wireless PIM synchronization. You can then view up-to-date handheld status information on the administration computer. Handheld status information can also be exported to the administration computer or to a network location.

Notes: C++-based handhelds report handheld information at the module level and not at the application level.

Handheld phone number and home network information can be reported on GPRS® and iDEN® handhelds only if a Subscriber Identity Module (SIM) card is inserted in the handheld and the handheld is provisioned for phone capabilities.

Configure handheld information management

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, double-click a user.
3. Click **PIM Sync**.
4. Perform one of the following actions:

Action	Procedure
Enable automatic handheld management.	1. Click **Automatic Handheld Management Enabled**. 2. From the drop-down list, select **True**.
Disable automatic handheld management.	1. Click **Automatic Handheld Management Enabled**. 2. From the drop-down list, select **False**.

5. Click **OK**.

View handheld status information from the configuration database

1. In the BlackBerry Manager, in the left pane, click **Handhelds**.
2. In the **User Name** list, click a user.

3. Click **View Handheld Properties**.

View handheld status information from the handheld

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click **Ports**.
3. In the **Connection** list, click a connection.
4. Click **View Handheld Properties**.

Retrieve handheld status information

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click **Ports**.
3. In the **Connection** list, click the handheld to retrieve handheld information from.
4. Click **Retrieve Summary Properties**.

Export handheld status information

1. In the BlackBerry Manager, in the left pane, click **Handhelds**.
2. In the **User Name** list, click a user.
3. Click **Export Asset Summary Data**.
4. Select a location to export the handheld data to.
5. Type a name for the handheld data file.
6. Click **Save**. The data is saved in a .csv or .txt file in the location that you specified in step 4.

Note: See "Appendix A: Exported handheld properties" on page 39 for a detailed description of the exported handheld information.

Set handheld owner information

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. In the right pane, expand **IT Admin**, and then click **Set Owner Information**.
4. Type the owner name and information.
5. Click **OK**.

Note: To prevent users from overwriting owner information, define the Set Owner Info and Lock Owner Info IT policy rules.

Controlling Handheld Software applications

You control Research In Motion (RIM) Handheld Software and third-party software applications from the administration computer by modifying the software configuration assigned to a user. You can install or remove the same software applications on multiple handhelds at the same time using the same software configuration. This method loads multiple handhelds while minimizing your interaction with the BlackBerry Manager.

You can also interact with the software application loading process for full control over the applications installed on or removed from individual handhelds. This method loads each handheld one at a time.

Define which applications are installed on handhelds

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. Perform one of the following actions:

Action	Procedure
Load the same software applications on multiple handhelds.	1. Create or modify a software configuration if desired. See "Set a software configuration" on page 16 or "Modify a software configuration" on page 27 for more information. 2. In the BlackBerry Manager, in the left pane, click **Ports**. 3. In the **Connection** list, click the desired connections. 4. Click **Load Handheld**. **Note:** If you select a handheld assigned to a user who does not have a software configuration defined, you are prompted to select a software configuration to use, but the software configuration is not assigned to the user.
Load software application on one or more handhelds interactively.	1. In the BlackBerry Manager, in the left pane, click **Ports**. 2. In the **Connection** list, click a connection. 3. Click **Load Handheld-Interactive**. 4. In the Welcome screen, click **Next**. 5. Type the security password for the handheld, and then click **Next**. 6. In the **Handheld Application Selection** screen, select the check box beside the applications to install on the handheld. 7. Clear the check box beside applications to remove from the handheld. 8. Click **Next**. 9. Click **OK**.

Controlling third-party software applications

You can send third-party applications to handhelds wirelessly. You can define and assign IT policies to users and application control policies to software configurations for additional administrative control over third-party applications on handhelds.

Application control policies define the specific resources that third-party applications can access on the handheld and behind the corporate firewall. Application control policies can also be used to make sure that third-party applications remain installed on handhelds and undesired third-party applications are removed from handhelds.

Third-party applications that are not assigned a specific application control policy are assigned the default application control policy that shipped on the handheld.

Note: You are solely responsible for the selection, implementation, and performance of any third-party applications that you use with the Handheld or Desktop Software. Research In Motion does not in any way endorse or guarantee the security, compatibility, performance, or trustworthiness of any third-party application and shall have no liability to you or any third-party for issues arising from such third-party applications.

Define IT policies for third-party applications

Set IT policies to permit third-party applications to be loaded onto handhelds or prevent the applications from being loaded.

1. In the BlackBerry Manager, on the **Global** tab, click **Edit Properties**.
2. Click **IT Policy**.
3. In the **IT Policy Administration** section, double-click **IT Policies**.
4. Click **New**.
5. Double-click **IT Policy Name**.
6. Type a new policy name.
7. Add the third-party application IT policy rules to the new policy.

IT policy rule	Settings	Default
Allow Third Party Apps to Use Serial Port	True, False	True
Allow Third Party Apps to Use Persistent Store	True, False	True
Desktop Allow Desktop Add-Ins	True, False	True
Disallow Third Party Application Downloads	True, False	False

8. Click **OK**.

Notes: See the *BlackBerry Enterprise Server for IBM Lotus Domino Administration Guide* for more information on creating and configuring IT policies.

For more control over individual third-party applications, define and assign application control policies. See " Define application control policies" on page 25 for more information.

Viewing the status of IT policy changes

When you apply an IT admin task or change the IT policy applied to a user, the status of the IT policy change displays in the BlackBerry Manager, in the **Policy Status** column.

Tip: To view the **Policy Status** column, move the scroll box to the right.

Status of IT policies	Description
Pending	This status indicates that there is new data waiting to be sent to the handheld and, or desktop.
Processing	This status indicates that the BlackBerry Enterprise Server is sending the change to the user. This status should not display for an extended period of time. If the status does not change within a short time, the status of the BlackBerry Enterprise Server might have changed while it was processing the request.
Sent	This status indicates that the IT policy change has been sent wirelessly to the handheld and, or desktop, but the user has not yet received the change.
Received	This status indicates that the handheld and, or desktop received the IT policy change, but the BlackBerry Enterprise Server has not received an error or a success message to indicate if the change has been applied.

Status of IT policies	Description
Applied successfully	This status indicates that the handheld and, or desktop received the IT policy change and successfully applied the change.
Error	This status indicates that an error occurred when the policy change was processed, sent, received, or applied.
Timed out	This status indicates that the IT policy change request timed out after 7 days. The handheld might be turned off or outside a wireless coverage area.

Sending IT policies to handhelds

If you assign a new policy to a user, that policy is sent automatically to the handheld.

Note: Sending a wireless IT policy creates a security association between the handheld and the BlackBerry Enterprise Server. After this association is made, the handheld does not accept IT policies from any other BlackBerry Enterprise Server or from the user computer through the serial port.

Resend an IT policy manually to a handheld

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. In the right pane, expand **IT Admin**, and then click **Resend IT Policy**.

Note: See the *BlackBerry Enterprise Server for IBM Lotus Domino Administration Guide* for more information on sending IT policies.

Define application control policies

You can define application control policies and load then onto Java-based handhelds that are running Handheld Software version 4.0. See "Appendix B: Software application control" on page 43 for more information.

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. Click **Manage Application Policies**.
3. Click **New**.
4. Type a new policy name.
5. Customize the application control policy properties.

   Tips: To make sure that a third-party application remains installed on a handheld, from the **Disposition** drop-down list, select **Required**.

   To remove a third-party application from a handheld, from the **Disposition** drop-down list, select **Disallowed**.
6. Click **OK**.

Assign application control policies to software configurations

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. From the **Configuration Name** list, click a software configuration.
3. Click **Edit Configuration**.

4. Expand the **Application Software** application tree.
5. From the **Policy** drop-down list, select an application control policy for the desired third-party application.
6. Click **OK**.

Tips: When you select an application control policy at the application software level, that policy becomes the effective policy for all third-party applications.

If you select **<default>** from the **Policy** drop-down list for a third-party application, the effective policy is assigned and an asterix is suffixed to the policy name.

Manage application control policies

When an application control policy is changed, the application control policy is resent automatically to the handheld wirelessly.

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. Click **Manage Application Policies**.
3. Perform one of the following actions:

Action	Procedure
Add an application control policy.	▸ See "Deploying handhelds using the administration computer" on page 18.
Modify an application control policy.	1. Click the application policy. 2. Click **Properties**. 3. Modify the application control policy properties. 4. Click **OK**.
Remove an application control policy.	1. Click the application policy. 2. Click **Remove**.

Send third-party software applications to handhelds wirelessly

You can send third-party applications wirelessly to Java-based handhelds with 16 MB of flash memory that are running Handheld Software version 4.0. When sending third-party applications to handhelds wirelessly, the wireless download can take up to 4 hours to complete.

To make sure that a third-party application remains installed on a handheld, create and assign an application control policy to the third-party application in the software configuration. See "Define application control policies" on page 25 for more information.

1. Install the third-party software application. See "Install Handheld Software" on page 34 for more information.
2. Verify that the software is installed in the shared network directory. See "Share Handheld Software and upgrade tools" on page 35 for more information.
3. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
4. In the **Configuration Name** list, click a software configuration.
5. Click **Edit Software Configuration**.
6. Expand the application, and then select the check boxes beside the applications to push wirelessly.

7. From the **Delivery** drop-down list, select **Wireless**.

   Tip: To make sure that a third-party application remains installed on a handheld, create and assign an application control policy, and from the **Disposition** drop-down list, select **Required**.

8. Click **OK**.

Managing software configurations

You manage software configurations using the administration computer on which the BlackBerry Manager is installed. If you delete a software configuration, it can no longer be assigned to a user. If you unassign a software configuration from a user, you cannot send application control policies to that user.

Modify a software configuration

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. In the **Configuration Name** list, click a software configuration.
3. Click **Edit Software Configuration**.
4. In the **Application Name** list, select the check box beside the applications to install on handhelds.
5. In the **Application Name** list, clear the check box beside the applications to remove from handhelds.
6. Click **OK**.

Tip: You can modify an application control policy while modifying a software cofiguration by clicking **Policies** in the Handheld Software Configuration window.

Delete a software configuration

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. In the **Configuration Name** list, click a software configuration.
3. Click **Delete Software Configuration**.
4. Click **OK**.

Copy a software configuration

1. In the BlackBerry Manager, in the left pane, click **Software Configurations**.
2. In the **Configuration Name** list, click a software configuration.
3. Click **Copy Software Configuration**.

Unassign a software configuration from a user

1. In the BlackBerry Manager, in the left pane, click **Handhelds**.
2. In the **User Name** list, click a user to assign the software configuration to.
3. Click **Assign Software Configuration**.
4. Click **<none>**.

5. Click **OK**.

Check the status of Handheld Software and third-party applications on a handheld

You can compare the Handheld Software and third-party applications installed on a handheld against the Handheld Software and third-party applications defined in the user's software configuration. You can also identify handhelds that are not running the most recent or desired version of Handheld Software.

1. In the BlackBerry Manager, in the left pane, click **Handhelds**.
2. In the **User Name** list, click a user.
3. Click **Update Configuration Check Status**.

The lower pane displays the following handheld configuration status information:

Status name	Description
Configuration Status	the overall status of the user's defined software configuration with respect to the software installed on the user's handheld
System Status	the status of the handheld's current Handheld Software with respect to the user's defined software configuration
Application Status	the status of the handheld's current third-party applications with respect to the user's defined software configuration

See the *BlackBerry Enterprise Server for IBM Lotus Domino Troubleshooting Guide* for more information on handheld configuration status messages.

Handheld security

To manage handheld security, you can set a new handheld password that replaces the existing password. This action locks the handheld and prompts the user for the new password. If the handheld has an existing password, a prompt alerts the user to accept the password. Users can accept the new password or continue to use their existing password.

You can disable a handheld and delete all of the information stored on that handheld, including application data. The handheld can later be re-enabled by a wireless activation or by activating the handheld and loading applications using the administration computer.

Manage handheld security

- Perform one of the following actions:

Action	Procedure
Set a password and lock the handheld.	1. In the BlackBerry Manager, in the left pane, click a server. 2. On the **User List** tab, click a user. 3. In the lower pane, expand IT Admin tasks, and then click **Set Password and Lock Handheld**. 4. In the **New Password** and **New Password Again** fields, type a password that is 4 to 14 characters long. **Warning:** Do not use special characters when you create the password. The BlackBerry handheld does not accept special characters. 5. Select the **Set Owner Information also** check box. 6. In the **Owner Name** and **Owner Information** fields, type the information. 7. Click **OK**.
Disable a handheld and delete stored information.	1. In the BlackBerry Manager, in the left pane, click a server. 2. On the **User List** tab, click a user. 3. In the lower pane, expand IT Admin tasks, and then click **Erase Data and Disable Handheld**. 4. Click **Yes**.
Delete handheld application data.	1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed. 2. In the BlackBerry Manager, in the left pane, click **Ports**. 3. In the **Connection** list, click a connection. 4. Click **Wipe Handheld File System**. 5. Click **Yes**. **Note:** A prompt alerts you to type the handheld password to complete this task.
Disable a handheld, and delete all applications and stored data.	1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed. 2. In the BlackBerry Manager, in the left pane, click **Ports**. 3. In the **Connection** list, click a connection. 4. Click **Nuke Handheld**. 5. Click **Yes**. **Note:** To restore functionality to the handheld, in the left pane, in the **Ports** section, click **Load Handheld**.

Managing activation passwords

If you generate and email an activation password to a user, and then set the activation password, you overwrite the existing activation password even if the activation period has not expired. Overwriting the activation password is useful for troubleshooting an individual handheld activation if the user cannot read the email that contains the original activation password. You must inform the user of the new password by phone or by manually sending an email message.

You can delete the activation password before the activation period has elapsed. The user cannot activate the handheld using that password.

Reset an activation password

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. Expand **Service Access**.
4. Click **Set Activation Password**.
5. Type a shared secret password.
6. Retype the password to confirm it.
7. From the **Password Expires in** drop-down list, select an expiration time.

   Note: Accented characters are not supported in activation passwords.

8. Click **OK**.

Expire an existing activation password

Note: You must know the existing active activation password to expire it.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. Expand **Service Access**.
4. Type the existing activation password.
5. Retype the password to confirm it.
6. From the **Password Expires in** drop-down list, select **0 hours (now)**.
7. Click **OK**.

Issuing new handhelds to users

Scenario	Procedure
Lost handheld	▸ Assign a new password and lock the handheld. See "Manage handheld security" on page 29 for more information.
Stolen handheld	▸ Disable the handheld and delete stored information. See "Manage handheld security" on page 29 for more information.

When a user receives a new handheld, you must register the new PIN for email redirection. If the user does not have access to the Desktop Software, register the new handheld using the BlackBerry Manager.

If users receive a replacement handheld, and they want to enable wireless calendar synchronization, they must enable it using the optional Desktop Software or configure it directly on the handheld. See the *BlackBerry Wireless Handheld User Guide* for more information. To activate the handheld wirelessly, the handheld must be running Handheld Software version 4.0.

Activate a new handheld

- Perform one of the following actions:

Action	Procedure
Activate a handheld connected to the administration computer.	1. Enable email pre-population if desired. See "Enabling email prepopulation" on page 17 for more information. 2. Assign the new handheld to the user. See "Assign a handheld to a user" on page 18 for more information.
Activate a handheld wirelessly.	1. Enable email prepopulation if desired. See "Enabling email prepopulation" on page 17 for more information. 2. Perform a wireless activation. See "Deploying handhelds wirelessly" on page 19 for more information. 3. Send users the path to the Application Loader tool or instruct users to run the backup and restore utility in the Desktop Manager. **Note:** When handhelds are deployed wirelessly, users must run the Application Loader or the backup and restore utility in the Desktop Manager to back up their handheld data to the database. See "Appendix C: Wireless backup and restore" on page 45 for more information.

Issuing existing handhelds to new users

You can issue an existing handheld to a new user using the administration computer or wirelessly. If you issue a handheld using the administration computer, the handheld must be connected to the administration computer.

If you issue a handheld wirelessly, the handheld does not have to be in your possession when you redistribute the handheld.

Switch the user account on the handheld

- Perform one of the following actions:

Action	Procedure
Redistribute a handheld using the administration computer.	1. Delete all handheld data. See "Manage handheld security" on page 29 for more information. 2. Assign the handheld to the new user. See "Assign a handheld to a user" on page 18 for more information.
Redistribute a handheld wirelessly.	1. Disable the handheld and delete stored information. See "Disable a handheld and delete stored information." on page 29 for more information. 2. Enable email prepopulation if desired. See "Manage handheld security" on page 29 for more information. 3. Perform a wireless activation. See "Deploying handhelds wirelessly" on page 19 for more information. **Note:** When users enter the activation password, they are prompted by the handheld to switch the email address and delete handheld data. 4. Send users the path to the remote Application Loader tool or instruct users to run the backup and restore utility in the Desktop Manager. **Note:** When handhelds are deployed wirelessly, users must run the Application Loader or the backup and restore utility in the Desktop Manager to back up their handheld data to the database. See "Appendix C: Wireless backup and restore" on page 45 for more information.

4

Upgrading handhelds

- Selecting an upgrade method
- Configuring Handheld Software on an administration computer
- Upgrading Handheld Software

Selecting an upgrade method

There are three different upgrade options that you can use to upgrade Handheld Software. If you upgrade Handheld Software using the administration computer or upgrade Handheld Software using the Application Loader, you must install the Handheld Software in a shared software directory on an administration computer. See "Configuring Handheld Software on an administration computer" on page 34 for more information.

If you upgrade Handheld Software using the Desktop Manager, the Handheld Software must be installed on user computers.

Upgrade options	Uses and advantages	Limitations
Upgrade Handheld Software using the administration computer	• use defined software configurations to quickly upgrade one or more handhelds at the same time • required if users do not have the Handheld Manager or the Desktop Manager installed on their computers • configure the Handheld Software installation for more uniformity in the applications that are installed on handhelds • remove unwanted software applications from handhelds • users do not have to install Handheld Software on their computers • upgrade a handheld that is not assigned to a user	• requires the handhelds to be connected to the administration computer on which the BlackBerry Manager is installed • the number of handhelds that you can upgrade at the same time is limited to the number of communication ports on the administration computer on which the BlackBerry Manager is installed
Upgrade Handheld Software using the Application Loader	• handhelds do not have to be upgraded using the administration computer • the Application Loader can be opened by multiple users to upgrade multiple handhelds at the same time • configure required software applications to be installed on handhelds • one instance of a Handheld Software version is installed and centrally stored in a shared software directory • users do not have to install the Handheld Software on their computers • users can perform a handheld backup and store the backup on their computer	• cannot make sure that users upgrade their handhelds after you have notified them to • cannot force users to remove unwanted software applications from their handhelds • cannot use software configurations to create uniformity in the applications that are installed on handhelds

Upgrade options	Uses and advantages	Limitations
Force Handheld Software upgrades to users using the Desktop Manager	• handhelds do not have to be upgraded using the administration computer • forces users to upgrade their Handheld Software • multiple users can upgrade their handhelds at the same time • users can perform a handheld backup and store the backup on their computer	• users must install the Handheld Software on their computers • cannot configure required software applications to be installed • cannot force users to remove unwanted software applications from their handhelds

Configuring Handheld Software on an administration computer

To upgrade Handheld Software, install the software upgrade from your service provider either on an administration computer that is running the BlackBerry Manager or on another computer.

After you install the Handheld Software on an administration computer, configure the Handheld Software. If you make a software upgrade required, the upgrade appears selected when users start the Application Loader. After you configure the Handheld Software, share the directory where the Handheld Software resides.

The Application Loader is provided both as a standalone program within the Handheld Software installation files and on the BlackBerry Enterprise Server. You must share the software loading tool from the computer on which you installed the software upgrade. This enables you to send a link to users who can start the Application Loader from the shared software directory without having to install the BlackBerry Desktop Manager.

The Application Loader searches the shared software directory for Handheld Software to install on handhelds. Users access the Application Loader from their computers to install handheld upgrades. You can use the BlackBerry Manager from a central location to load Handheld Software onto handhelds.

Install Handheld Software

▸ Perform one of the following actions:

Action	Procedure
Install Handheld Software.	1. Click the **.exe** file on the administration computer that hosts the shared software. 2. Complete the installation. **Note:** Verify that the files are located in *<drive:>*\Program Files\Common Files\Research In Motion\Shared\Loader Files\.
Install third-party software applications.	1. Create the directory *<drive:>*\Program Files\Common Files\Research In Motion\Shared\Applications\. 2. Copy the **.alx**, **.cod**, and **.dll** files to a unique subdirectory in the Applications folder, which preserves the subdirectory structure of the third-party application. **Note:** If the third-party vendor requires the application to be installed, complete the installation as instructed by the third-party vendor, and then copy the required application and module files to the Applications folder.

Tips: To locate third-party applications on the computer, open the Application Loader. On the Handheld Application Selection screen, click the application, and then click **Details**.

Maintain the shared software directory by removing old versions of Handheld Software. See "Maintain Handheld Software in the shared software directory" on page 36 for more information.

Configure required software

Warnings: Changing the software .alx file overwrites the application settings defined in the software configuration or in the Application Loader.

If <required>true</required> is added to a software .alx file, the software application cannot be removed from the handheld.

1. Open the **.alx** file that is associated with the installed Handheld Software application.
2. Perform one of the following actions:

Action	Procedure
Configure required Handheld Software.	1. Below the line <copyright>Copyright 1998-2004 Research In Motion</copyright>, type **<required>true</required>**. 2. Save the **.alx** file.
Configure required third-party applications.	1. Within the <application> element, type **<required>true</required>**. 2. Save the **.alx** file.

Note: Make sure that the handheld you are deploying Handheld Software upgrades to has sufficient storage space to accommodate all of the Handheld Software applications and third-party applications that contain the <required>true</required> element. If a handheld has insufficient space during the upgrade, the upgrade fails.

Create the software index

For the Application Loader to locate software to install, the Handheld Software must be indexed on the administration computer that hosts the shared software. The Application Loader reads the list of installed software from the index and displays it in the Handheld Application Selection window. Each software bundle generates the following index files:

- specification.pkg
- PkgDBCache.xml

Note: You must create the software index for third-party applications, Java-based Handheld Software versions 3.6 and newer (excluding 4.0), and C++-based Handheld Software versions 2.0 and newer (excluding 2.7).

1. At the command prompt, type **cd %CommonProgramFiles%\Research In Motion\Apploader**.
2. Type **loader.exe/index**. The Application Loader builds the directory structure in the shared software directory and adds any missing index files for installed software upgrades.

Tips: If you modify an **.alx** file after creating a software index, re-index the Handheld Software. At the command prompt, type **cd %CommonProgramFiles%\Research In Motion\Apploader**. Type **loader.exe/reindex**.

Run the Application Loader locally to verify that the required applications are selected in the Handheld Application Selection screen.

Share Handheld Software and upgrade tools

1. Verify that the handheld upgrade software is installed in *<drive:>*\Program Files\Common Files\Research In Motion.
2. Share *<drive:>*\Program Files\Common Files\Research In Motion.
3. Set the permission attributes to **Read-only**.

Note: The Handheld Manager must be installed on user computers. The Application Loader connects to a BlackBerry handheld. See "Configuring the BlackBerry Desktop Software installation files" on page 11 for more information on deploying the Handheld Manager to user computers.

Verify that the Application Loader is shared

1. Connect a handheld to the administration computer.
2. At the command prompt, type *<shared computer name>*\Research In Motion\Apploader\loader.exe.

   If the Application Loader starts, the tool is shared successfully.

Maintain Handheld Software in the shared software directory

1. Open the Control Panel, and then click Add/Remove Programs.
2. Click the version of Handheld Software to remove.
3. Click Remove.

Maintain third-party applications in the shared software directory

- Perform one of the following actions:

Action	Procedure
Remove third-party applications installed on the administration computer.	1. Open the Control Panel, and then click **Add/ Remove Programs**. 2. Click the version of Handheld Software to remove. 3. Click **Remove**.
Remove third-party application files copied onto the administration computer.	1. Browse to *<drive:>*\Program Files\Common Files\Research In Motion\Shared\Applications. 2. Delete the subdirectory folder where the third-party application resides.

Upgrading Handheld Software

After you select an upgrade method and configure the Handheld Software, you can upgrade handhelds with the new software. To upgrade handhelds at the administration computer without interacting with the Handheld Software loading process, a software configuration must be defined. See "Set a software configuration" on page 16 for more information.

Notes: You can upgrade a handheld that is not assigned to a user.

You can send third-party software applications wirelessly to user handhelds. See "Send third-party software applications to handhelds wirelessly" on page 26 for more information.

Upgrade handhelds using the administration computer

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click Software Configurations.
3. In the Configuration Name list, click Edit Software Configuration.
4. In the Applications List, select the check box beside the handheld series to upgrade Handheld Software for.
5. Expand the handheld series Handheld Software application tree.
6. From the Version drop-down list, select the version of Handheld Software to install.

   Note: If only one version of Handheld Software resides in the shared software directory, this drop-down list is unavailable.

7. Click **OK**.
8. In the left pane, click **Ports**.
9. In the **Connection** list, click the handheld to load the Handheld Software upgrade to.

   Note: If you select a handheld that is assigned to a user who does not have a software configuration defined, you are prompted to select a software configuration to use, but the software configuration is not assigned to the user. See "Assign a software configuration to a user" on page 18 for more information.

10. Click **Load Handheld**.

Tip: To interact with the Handheld Software loading process, click **Load Handheld-Interactive**.

Upgrade handhelds using the Application Loader

To upgrade handhelds that are connected to user computers, the Handheld Manager or Desktop Manager must be installed on the computers. See "BlackBerry Desktop Software" on page 10 for more information.

The Application Loader requires a physical connection to the handheld.

- Use your preferred distribution method (for example, a link in an email or a link on a web site) to send users the following UNC path to the location of the Application Loader: *<shared computer name>*\Research In Motion\Apploader\loader.exe.

When users click the link, the Application Loader starts and looks in the shared software directory for software upgrades to install. The Application Loader caches the Handheld Software upgrade on each user computer in case network interruptions occur during the upgrade.

Note: Users are prompted to perform a backup of their handhelds when the installation completes. See "Appendix C: Wireless backup and restore" on page 45 for more information.

Forcing upgrades to handhelds using the Desktop Manager

To upgrade Handheld Software using the Desktop Manager, user computers must have the handheld software upgrade installed. Distribute the Handheld Software installation package to user computers using your preferred distribution method.

You can force users to upgrade their Handheld Software by defining forced handheld upgrading IT policies. These IT policies define the number of times that users can restart the Desktop Manager before they are forced to run the Application Loader and upgrade their handheld applications.

Policy rule	Description	Default
Force Load Count	This rule specifies the number of times that a user can decline a software upgrade before the update is forced.	No limit
Force Load Message	This rule specifies the message that appears when users are prompted to update to a later version of Handheld Software.	NULL

Set forced upgrade IT policies

1. In the BlackBerry Manager, on the **Global** tab, click **Edit Properties**.
2. Click **IT Policy**.
3. In the **IT Policy Administration** section, double-click **IT Policies**.

4. Perform one of the following actions:

Action	Procedure
Add a rule to the default policy.	1. From the list of policies, click **Default**. 2. Click **Properties**.
Create a new IT policy.	1. Click **New**. 2. Type a policy name.

5. Click the **Desktop-Only Items** policy group, and then double-click the **Force Load Count** policy rule.
6. Type the number of prompts before users must upgrade their Handheld Software.
7. In the **Desktop-Only Items** policy group list, double-click the **Force Load Message** policy rule.
8. Type the message to appear when new software is available.
9. Click **OK**.
10. Perform one of the following actions:

Action	Procedure
Send the modified default policy to users.	1. Click **OK**. 2. Click **OK** again.
Add users to a new policy and send the policy to selected users.	1. In the **IT Policy Administration** section, double-click **IT Policies**. 2. In the left pane, click a user. 3. In the right pane, click the new policy. 4. Click **OK**.

Note: See the *BlackBerry Enterprise Server for IBM Lotus Domino Administration Guide* for more information on creating and configuring IT policies.

Appendix A: Exported handheld properties

- Handheld hardware components
- Handheld software components
- Component capabilities
- Status
- Service books
- Software applications
- Modules

Handheld hardware components

Component	Description
PIN	the handheld PIN number
Handheld Model	the model version of the BlackBerry Wireless Handheld
Network Type	the network that the handheld is connected to, for example, GPRS
Memory	the total amount of memory shipped on the handheld
Serial Number	the handheld electronic serial number
Frequencies	the wireless frequencies supported by the handheld
Carrier	the wireless carrier who provided the handheld
Secured Boot ROM	a secured boot ROM that allows only signed RIM system software to be loaded on handhelds **Note:** This value is set to **TRUE** for Java-based handhelds and **FALSE** for C++-based handhelds.
Display Screen width	the width of the handheld display screen in pixels
Display Screen height	the height of the handheld display screen in pixels

Handheld software components

Component	Description
Last Update Time	the date and time of the last handheld data update
Platform Version	the handheld operating system version
BlackBerry Version	the BlackBerry Wireless Handheld software version
Phone Number	the phone number assigned to the handheld **Note:** This component is not available for C++-based handhelds and handhelds that are not provisioned for the phone application.
Security Password	indicates if a security password is set on the handheld
Home Network	identifies the home network for the handheld
Direct Connect ID	the Direct Connect ID for the handheld, if available **Note:** This component is not available for handhelds on iDEN networks.
IT Policy Name	the name of the IT policy assigned to the handheld
IT Policy Time	the time when the IT policy was loaded onto the handheld

Component capabilities

Capability type	Component	Description
General capabilities	Wireless PIM Data Synchronization	specifies whether the handheld supports wireless PIM synchronization
	Sent Items Synchronization	specifies whether the handheld supports wireless synchronization of the Sent Items folder
	Wireless Application Delivery	specifies whether the handheld supports wireless application delivery
	Application Control Policies	specifies whether the handheld supports control over third-party applications by application control policies
Security capabilities	S/MIME	specifies whether the handheld supports S/MIME-encoded email
	PGP	specifies whether the handheld supports PGP-encoded email
	Encryption Algorithms	the encryption algorithms that the handheld supports
Character encoding capabilities	Email Encodings	the encodings that the handheld supports for wireless email delivery
	Calendar Encodings	the encodings that the handheld supports for wireless calendar operations
	Address Lookup Encodings	the encodings that the handheld supports for wireless address book look up operations
	PIM Synchronization Encodings	the encodings that the handheld supports for wireless PIM synchronization

Status

These components values are updated every 6 hours.

Component	Description
Last Update Time	the date and time of the last Handheld Software update
Available Memory	the amount of memory available on the handheld
Battery Level	the amount of battery life on the handheld
Uptime	the length of time that the handheld has been turned on

Service books

Component	Description
Content ID	the data content managed by the selected service book entry
Service ID	the server endpoint for the selected service book entry
Service Data	the application-specific data for the selected service book entry **Note:** This information is used by Technical Support to troubleshoot service book problems.

Software applications

Component	Description
Description	the vendor description of the application
Version	the vendor-assigned application version
Vendor	the vendor of the handheld application
Copyright	the application copyright notice

Modules

Component	Description
Version	the version of the handheld application module
Size	the size of the handheld application module in bytes

Appendix B: Software application control

- Application control policy properties
- Sample application control policies
- Sample software configurations

Application control policy properties

Property	Description	Default value
Internal Domains	the internal domain names to which the application can establish a connection	NULL
External Domains	the external domain names to which the application can establish a connection	NULL
Browser Filter Domains	the browser filter domain list	NULL
Disposition	controls whether the application is optional, required, or not permitted on the handheld	Optional
Interprocess Communication	controls whether the application can perform interprocess communication operations	Allowed
Internal Network Connections	controls whether the application can make internal network connections	Prompt User
External Network Connections	controls whether the application can make external network connections	Prompt User
Local Network Connections	controls whether the application can make local network connections	Allowed
Phone Access	controls whether the application can initiate telephone calls	Prompt User
Email Access	controls whether the application can send and receive email messages	Allowed
PIM Data Access	controls whether the application can access the handheld PIM APIs	Allowed
Browser Filters	controls whether the application can register a browser filter with the browser	Not Permitted
Event Injection	controls whether the application can inject synthetic input events, such as keypress and trackwheel actions	Not Permitted
Bluetooth Serial Profile	controls whether the application can access the Bluetooth® serial profile API	Allowed
Handheld Keystore	controls whether the application can access the handheld keystore APIs	Allowed
Handheld Keystore Medium Security	controls whether the application can access key store items stored at the medium security level	Allowed

Sample application control policies

Consider the following scenarios when defining your own third-party application control policies:

Control scenario	Rules to set	Values to set
Make sure a third-party application remains installed on a handheld.	Disposition	Required

Control scenario	Rules to set	Values to set
Do not allow a third-party application to be loaded onto a handheld.	Disposition	Disallowed
Permit a third-party application to connect to the internal domain to access internal resources behind the corporate firewall on the handheld and enable the user to achieve internal network connections (for example, Mobile Data Service) by prompting for a password.	Internal Network Connections	Prompt User
	Internal Domains	Type the address of the internal company domain
Prevent a third-party application from accessing a list of domains with the BlackBerry Browser.	Browser Filter domains	Type the address of the domains
Permit a third-party application to send and receive email on a handheld.	Email Access	Allowed
Remove a third-party application from a handheld.	Disposition	Disallowed
Allow a third-party application (for example, customer relationship management applications) to access the Phone application.	Phone Access	Allowed
Permit a third-party application to achieve public external network connections (for example, TCP, Bluetooth, or WAP Browser) and to allow a connection to external domains without prompting the user for a password.	External Network Connections	Allowed
	External Domains	Type the address of the external domains
Permit a third-party application to establish connections. to a Bluetooth-enabled device.	Bluetooth Serial Profile	Allowed
	External Network Connections	Allowed

Sample software configurations

Consider the following scenarios when defining your own handheld software configurations:

Configuration scenario	Procedure
Permit the phone, browser, and memopad to be loaded onto a handheld and remove the BlackBerry Attachment Service from a handheld.	1. Select the **Phone**, **Memopad**, and **Browser** check boxes. 2. Clear the **BlackBerry Attachment Service** check box.
Permit third-party applications to be sent wirelessly to a handheld and set the application to remain installed on the handheld.	1. Create an application policy in which the **Disposition** is set to **Required**. 2. Select the check boxes beside the third-party applications. 3. From the **Delivery** drop-down list, select **Wireless**. 4. From the **Policy** down-down list, select the application control policy.
Configure a Handheld Software application so that it must be installed on the handheld when users upgrade their handheld using the Application Loader.	1. Make the Handheld Software application required by configuring the application .alx file. 2. Update the software configuration to verify that the changes made to the configuration are correct.

Appendix C: Wireless backup and restore

- Data that is not backed up wirelessly
- Backup and restore handheld data

Data that is not backed up wirelessly

When handhelds are deployed wirelessly and Wireless Automatic Backup is enabled for a user, the following handheld data is not backed up:

Data	Description
Email messages	email messages received on the handheld before the specified prepopulation date, or that are located in folders not set for redirection, or that have email filters assigned to prevent redirection to the handheld
Content store	saved images and ring tones
Service books	all service books
Group addresses	group addresses created on the handheld are stored locally on the handheld only and are not synchronized
MMS messages	messages sent by MMS are stored locally on the handheld only
SMS messages	messages sent by SMS are stored locally on the handheld only
Saved messages	messages saved on the handheld
PIN messages	PIN messages are stored locally on the handheld only
RMS databases	third-party applications created in the J2ME™
Wirelessly downloaded third-party applications	third-party applications that are sent wirelessly to handhelds **Note:** Third-party applications can be restored to handhelds if the **Delivery** setting is set to **Wireless** in the user's software configuration.

Backup and restore handheld data

To back up data not backed up wirelessly, users must use the backup and restore utility in the Desktop Manager or run the Application Loader tool that is installed in the shared software directory to back up their handheld data on the database. Running a full backup creates an .ipd file on the user's computer.

An .ipd file typically saves as LoaderBackup-<*yyyy-mm-dd*>.ipd where *yyyy* specifices the year, *mm* specifies the month, and *dd* specifies the day of the backup. The .ipd file is typically found in C:\Documents and Settings\<*userid*>\My Documents where <*userid*> the user's ID.

Backup handheld data using the Application Loader

To backup handheld data to user computers, the Handheld Manager or Desktop Manager must be installed on user computers. The Application Loader requires a physical connection to the handheld. You can verify that the Application Loader is installed in the shared software directory on the administration computer on which Handheld Software is installed.

1. Connect a handheld to an administration computer with a connection to the network.
2. At the command prompt, type ***<shared computer name>*\Research In Motion\Apploader\loader.exe**. If the Application Loader starts, the tool is shared successfully.
3. Use your preferred distribution method (for example, a link in an email or a link on a web site) to send users the following UNC path to the location of the Application Loader tool: ***<shared computer name>*\Research In Motion\Apploader\loader.exe**.

When users click the link, the Application Loader starts and permits you to install Handheld Software on the handheld, and then prompts you to allow a backup of the handheld to be performed. When users accept the backup to be performed, the Application Loader produces a LoaderBackup-<*yyyy-mm-dd*>.ipd file, which contains all handheld data. This file is saved locally on the user's computer.

©2004 Research In Motion Limited
Published in Canada.